



EXECUTIVE OFFICE OF THE PRESIDENT

OFFICE OF MANAGEMENT AND BUDGET

WASHINGTON, D.C. 20503

March 24, 1978

o/c-78-0650

LEGISLATIVE REFERRAL MEMORANDUM

TO: Legislative Liaison Officer
Department of Justice
Federal Communications Commission
Department of the Treasury
Department of Defense
Central Intelligence Agency

SUBJECT: OTP (Commerce's National Telecommunications Information Administration) proposed report on H.R. 7341, "TELECOMMUNICATIONS PRIVACY ACT."

The Office of Management and Budget requests the views of your agency on the above subject before advising on its relationship to the program of the President, in accordance with OMB Circular A-19.

A response to this request for your views is needed no later than cob, Friday, April 21, 1978.

Questions should be referred to Bob Carlstrom (395-3856) or to _____ the legislative analyst in this office.

Bernard H. Martin for
Assistant Director for
Legislative Reference

Enclosures
cc: Mr. Neustadt

Mr. Bedell
Mr. Haase

GENERAL COUNSEL

March 13, 1978

Honorable Harley O. Staggers, Chairman
Committee on Interstate and Foreign Commerce
House of Representatives
Washington, D.C. 20515

Subject: H.R. 7341, "Telecommunications Privacy Act of 1977"

Dear Mr. Chairman:

OTP has reviewed the bill H.R. 7341 and, subject to the reservations discussed below, endorses enactment.

There are currently two basic federal laws dealing with communications privacy: Section 605 of the Communications Act of 1934,^{1/} and Chapter 119 of the Omnibus Crime Control and Safe Streets Act of 1968. ^{2/} OTP has long contended that these laws are inadequate to fully protect communications privacy. This inadequacy stems in part from archaic technological assumptions--an example being the definition of intercept in 18 USC §2510(4) as the aural acquisition of the content of any wire or oral communications. This definition ignores the importance of the knowledge of the existence of communications and patterns of communications in an information society (pen registers), and fails to take cognizance of modern non-aural methods of transmitting communications. Another weakness in the current law, recognized by the National Commission for the Review of Federal and State Laws Relating to Electronic Surveillance, derives from inadequate judicial enforcement of statutory restrictions on the authorizations of wiretapping and inefficient use of wiretapping as a law enforcement device. ^{3/} H.R. 7341 would amend current law by striking Chapter 119 from the Omnibus Act and replacing it with an updated version, more highly protective of communications privacy, as an addition to the Communications Act. Many of the provisions of Chapter 119 have been transferred intact.

^{1/} 47 USC §605.

^{2/} 18 USC §§2510 et. seq.

^{3/} H. Schwartz, Taps, Bugs, and Fooling the People (June 1977)

The major changes proposed by the bill are:

1. Extension of broadened intercept sanctions to all communications, without regard for the mode of transmission or manner of interception, when there is a legitimate expectation of privacy;
2. Extension of intercept sanctions and court order requirements to U.S. Government interception of the communications of U.S. citizens or nationals overseas;
3. Requirement of Federal court authorization for all interceptions requested by state law enforcement officials;
4. Limitations of the types of crimes for which interceptions may be authorized, and elimination of the use of intercepts for purely intelligence-gathering activities;
5. Restrictions on the circumstances under which information obtained from a legitimate interception may be disclosed;
6. Improved minimization and notification procedures designed to ensure that authorized intercepts are conducted in the least intrusive manner possible;
7. Amendment of the concept of "consensual" interceptions so that law enforcement officials and communications common carriers could not intercept without a court order or consent of both parties;
8. Elimination of the "good faith" defense to a civil action brought for violation of privacy in contravention of the intercept statute.

OTP supports action in all of these areas as a meaningful way to ensure the greatest possible privacy for the individual against government and private sector intrusion by more strictly delineating those circumstances under which society recognizes interception of communications to be legitimate. However, there are several proposed restrictions and safeguards which may be overly strict and may therefore unnecessarily hamper acceptable law enforcement and private sector activity. These are dealt with below.

Disclosure: Section 701

This section would restrict disclosure, in any form, of protected information obtained in a valid interception, to that information relevant to the purpose for which the intercept was authorized. Protected information is defined in Section 711 as information concerning the identity of a

party to a protected communication, or the existence of, or the contents of, such communications. Therefore, under section 701, any evidence of an unrelated crime, inadvertently discovered during the course of a properly authorized intercept, could be disclosed only subsequent to authorization for such disclosure by another court order. The rationale behind this restriction is that stringent oversight functions are necessary to ensure that intercepts are utilized only for specifically authorized purposes and not for general searches. OTP recognizes that the difficulty in protecting against abuse of authorized intercepts is a legitimate concern. Adoption of the approval and minimization standards proposed in this bill, and a Congressional mandate for more rigorous court review of intercept requests should go a long way towards accomplishing this goal. While the primary place to prevent "fishing expeditions" and similar abuses is at the point the intercept is authorized, additional safeguards are required. However, we do not believe that the requirement of a second court order is a viable oversight mechanism.

The Supreme Court has held that evidence of a crime inadvertently discovered during a proper search, may be used by police and disclosed in court. ^{4/} Therefore, the scope of the hearing for a second order would probably be limited to the issues of whether the intercept was conducted in accordance with the intercept authorization, and whether the secondary evidence obtained was indeed inadvertent. As an ex parte hearing, this could easily become a perfunctory procedure requiring little more than a sworn statement by law enforcement officials that they were in compliance. The following is offered as an example of a more effective approach.

When evidence of a secondary crime is inadvertently discovered during an authorized intercept, the person in charge of the intercept operation should be required to immediately submit to the proper court a transcript of the intercepted evidence, and a sworn affidavit to the effect that the discovery of such "ancillary" evidence was not an intended but undisclosed objective of the initial intercept request, and that the intercept had been conducted within the parameters of the intercept order. These documents would be kept in court custody. The evidence could then be used as the basis for further investigation.

^{4/} Coolidge v. N.H., 403 U.S. 433 (1971).

However, before submission to the Grand Jury, or after information but before arrest or arraignment based upon the "inadvertently obtained evidence" or its product, a hearing would have to be held in which the veracity of the affidavit mentioned above could be contested. If it is determined that the original evidence was not obtained inadvertently or that it was obtained because the intercept was not conducted in compliance with the terms of the court authorization, then the evidence would be inadmissible for all purposes. Furthermore, all evidence obtained in investigations which resulted from the "inadvertant" discovery would also be inadmissible as "fruit of the poisonous tree".5/

Notification Procedures: Section 708(i)

The bill would require notification of the approval or denial of authorization to intercept within 90 days of certain events. Extensions could be granted for up to 270 days upon a showing of good cause. At the end of that time, there must be notification to the proposed subject of the intercept. This standard makes no differentiation between foreign intelligence operations and domestic law enforcement activities. It is foreseeable that, in a limited number of foreign intelligence efforts, notification could endanger national security. Therefore, although OTP believes that virtually all authorizations for government interception of personal communications should be based upon a showing of probable cause that a crime has been committed and that evidence thereof will be obtained by the intercept, different procedural requirements for conducting foreign intelligence intercepts may be necessary to ensure an efficient foreign intelligence capability. This is especially evident regarding notice procedures.

Further, while OTP supports the use of a standard which requires the demonstration of criminal activity prior to authorization of an intercept for foreign intelligence purposes, we also recognize that there may be some extremely rare and unusual circumstances under which a lesser standard would be necessary to protect the nation's security. 6/

5/ This statutory treatment would be consistent with Fourth Amendment treatment of improperly obtained evidence under the Wong Sun doctrine. Wong Sun v. U.S. 371 U.S. 471(1963)

6/ OTP recognizes the concern many people have over the vagueness of the term "national security". We suggest that any exceptions to the criminal standard for a warrant be confined to the foreign intelligence area and very narrowly defined.

This predicament is embodied in the current debate regarding H.R. 1566. We do not believe that H.R. 7341 adequately addresses this concern and therefore, suggest that provisions be made for special consideration of these exigent circumstances on a case by case basis either by amendment of the proposed bill or by deferring to the proposed legislation in the foreign intelligence area.

Prohibition of Certain Activities Relating to Devices:
Section 702

Section 702 would make unlawful the manufacture or possession of any device primarily useful for surreptitious interception of protected communications. This provision is virtually identical to existing law. 7/ However, under section 711 of the proposed bill, "protected communications" means:

- (1) "a transfer of verbal, symbolic, or other information between persons or information processing facilities, including associated, switching, and signaling information--
"(A) that is made in whole or in part by wire, cable, microwave radio, satellite, or an optical system furnished or operated by a communications common carrier;
"(B) that is made on a private communication system; or
"(C) that is an oral communication uttered by a person having an expectation, in circumstances justifying that expectation, that such communication is not being intercepted.
- (2)(A) And the term "intercept" means to acquire protected information by means of any device, unless such acquisition is --
"(i) by a person who has the consent of all parties to that communication; or
"(ii) by a person who is not an employer of any party to that communication and not a law enforcement officer and who has the consent of one of the parties to that communication.
"(B) for the purposes of subparagraph (A) of this paragraph, consent shall not be implied from an employment relationship, nor shall any consent that is a condition of employment or a condition for the use of a private communication system be valid."

7/ 18 USC §2512.

Under these broad definitions many devices with legitimate and beneficial applications could be considered contraband. As an example, football broadcasts often utilize sound focusing devices to "intercept" and broadcast conversations of the players to the viewing audience. Further, the versatility of modern electrical devices and techniques makes it virtually impossible to determine whether they are "primarily useful" for surreptitious interception of protected communications.

Section 702 and 703 should be retained only if provisions can be made to ensure that legitimate and beneficial uses of technology will not be discouraged.

Consensual Interception: Section 711

By definition in Section 711, this bill would require law enforcement officials to obtain a court order authorizing an intercept even though one of the parties to the communications had consented. This is a departure from traditional theory, and the Supreme Court has held that such a provision is not mandated by the Constitution. ^{8/} However, OTP believes the safeguard of judicial overview in all circumstances is the only effective means by which abusive or unnecessary interceptions can be prevented. Furthermore, because this type of activity is often planned in advance, the burden placed on law enforcement officials is slight and increases only as their justification for intercept decreases. We do suggest however, that provisions be made for an exception to the court order requirement where exigent circumstances can be shown. This seems a proper balance to strike in a society dedicated to ensuring that its citizens are free from unreasonable government intrusion.

Service Observing: Section 708(k)

H.R. 7341 proposes that communications common carriers and operators of private communications systems be allowed to conduct Service Observing, that is, the monitoring of calls to assess the quality of telecommunications service rendered, only after justifying the need for such practices before a federal judge and obtaining a court order. This bill also provides certain procedural safeguards to apply when the intercepts are permitted (e.g., mandatory

^{8/} U.S. v. White, 401 U.S. 745 (1971); U.S. v. Palazzo, 478 F. 2d 942 (C.A. Tex. 1974).

publishing of the fact of such practices in local newspapers so that the public may be forewarned in its dealings with the carriers and operators). 9/ OTP has previously indorsed the concept that Service Observing should only be allowed after a showing that it is necessary and that no less drastic means is available to the applicant. We therefore support these provisions of the bill.

In addition, the following additional safeguards are suggested:

- Intercepts, when permitted, should not begin until thirty seconds after a call is placed, thus preventing discernment of the number dialed and giving the parties time to identify themselves before the intercept begins;
- Publication of the fact of intercept practices should be repeated periodically where Service Observing is an ongoing practice of the carrier or operator.

Supervisory Observing

The bill in its current form makes no realistic provisions for Supervisory Observing (i.e., monitoring calls for purposes of training or evaluation of employee performance). Under the provisions of this bill an employer is not allowed to apply for a court order to conduct such an intercept, nor does OTP believe a court order should be required. However, under the provisions of Section 711 of the bill, an employer could not conduct such a program without consent of both parties to the call. This would have the practical affect of preventing most Supervisory Observing. Also, consent could not be made a condition of employment and would have to be actual, not implied. While OTP agrees that there should be actual and informed consent, we believe that the other provisions in this regard place undue restrictions on the rights of business people to prescribe conditions of employment and to protect their business interests through the use of Supervisory Observing.

9/ An alternative and possibly more effective approach to newspaper publication would be to require publication along with the listing in the telephone directory.

We therefore suggest that provisions be made to allow Supervisory Observing either by an addition to the bill or by deleting the words...by a person who is not an employer of any party to that communication...in Section 711(2)(A)(ii) from the bill. In addition, the following safeguards should be required where Supervisory Observing is allowed:

- The employer should be required to publish notice of the practice.
- Where personal calls are allowed, the employer should be required to make some reasonable arrangement by which the calls could be placed and received without the possibility of monitoring.

Finally, we agree with the provisions of this bill insofar as they ban all eavesdropping of employees by employers.

In all other respects, OTP supports enactment of H.R. 7341.

Sincerely,

Gregg P. Skall
Acting